New York State Comptroller
THOMAS P. DiNAPOLI

Red Hook Central School District

Building Access

July 2026 | Report S9-26-7

Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Red Hook Central School District

Audit Objective

Did Red Hook Central School District (District) officials properly manage and monitor building access accounts and devices?

Audit Period

July 1, 2024 – November 30, 2025

We extended our audit period to January 21, 2026 to review access activity logs during our fieldwork.

Understanding the Audit Area

Building access controls are essential for enhancing security and enabling school officials to manage and monitor entry points within educational institutions. These systems authenticate a user through devices such as key fobs, keycards, badges, or similar technologies, helping to ensure only authorized individuals can enter school buildings. By limiting access in this way, schools can better safeguard their facilities and maintain a safe and secure environment for students, teachers, staff and visitors.

The District utilizes a building access management system (system) with 827 active building access accounts (accounts), including 457 devices issued to current employees, and 370 issued to non-employees of which 17 are shared devices.[1] Each of the District's three school buildings has one public point of entry. Employees may also access the buildings through additional secured entry points, which require a device for entry.

Audit Summary

District officials did not properly manage and monitor building access accounts and devices (badges). As a result, there was a potential risk for unauthorized access to District school buildings, compromising building security and safety for students, teachers, staff and visitors. Specifically, of the accounts we reviewed, the District had active, but unneeded, accounts with assigned badges in the system:

- 37 District employees and 19 non-employees had at least two active badges.
- 28 non-employee badges were not disabled when no longer needed. These included badges assigned to former employees, consultants and police officers, as well as three individuals that District officials did not recognize.

Although the District had a Board-established policy for issuing badges, including procedures for replacement and access modification, it was outdated and did not align with the District's actual practices during the audit period. Additionally, there was no regular access review, and District officials neither assigned clear responsibility for account oversight nor ensured access request documentation was retained.

This report includes six recommendations that, if implemented, will help District officials and the Board of Education (Board) improve management and monitoring of building access accounts and badges. District officials generally agreed with our recommendations and their response is included in Appendix B.

1 A shared account or device is assigned to a user for a specific role or function but not assigned to a specific individual (e.g., vendors or first responders).

This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's (OSC's) authority as set forth in Article 3 of New York State General Municipal Law (GML). This audit's methodology and standards are included in Appendix C.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to OSC within 90 days, pursuant to Section 35 of the New York State General Municipal Law (GML), Section 2116-a (3)(c) of the New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing the CAP, please refer to the OSC brochure, *Responding to an OSC Audit Report*, which was provided with the draft audit report. The CAP should be posted on the District's website for public review.

Building Access: Finding and Recommendations

Properly managing and monitoring building access is a fundamental security function and the responsibility of school district officials. Various resources, publications, and guides are available to help school district and Board of Cooperative Educational Services (BOCES) (together, “schools”) officials develop and implement necessary building access infrastructure and systems to create a safe and secure environment for their students, teachers, staff and visitors.

To issue accounts and badges, the District used a badge application form that required:

- Details about the individual requiring a badge (i.e., the reason for access, locations, time restrictions, etc.), and
- Authorizing signatures from the respective department head or administrator responsible for the employee, vendor or reason for the request.

More details on the criteria used in this report, as well as resources we make available to local officials that can help them improve operations, are included in Appendix A.

Finding 1 – District officials did not properly manage and monitor building access accounts and badges.

During our fieldwork in January 2026, the District had 827 active accounts associated with 457 badges issued to 420 current employees, and 370 badges issued to non-employees including 353 to individuals and 17 shared badges. We determined:

- 9 percent of current employee accounts had duplicate active badges,
- 6 percent of non-employee accounts had duplicate active badges, and
- 82 percent of non-employee accounts we reviewed were not needed.

<u>Employee Accounts</u> – Of the 420 current employees, 37 employees (9 percent) were assigned two active badges. For a sample of four of these employees, we reviewed four badge application forms. The badge application forms indicated that each new badge was issued as a replacement for a damaged or lost badge. However, a new account and associated badge was created instead, resulting in duplicate active accounts and badges. In addition, none of the badge application forms we reviewed had authorizing signatures and two were incomplete (e.g., previous badge number not documented).

<u>Non-Employee Accounts</u> – Of the 353 individual non-employee badges assigned to 333 individuals, 19 individuals (6 percent) were assigned two or more active badges, including one individual with three active badges. We reviewed a sample of four individuals, including the individual with three active badges, for a total of nine badges. We determined seven badges were issued to former third-party contractors who no longer provided services to the District, and two badges were associated with a former employee. As with the duplicate employee badges, the badges were issued as new badges instead of replacements for damaged or lost badges, resulting in duplicate active accounts and badges.

In addition, we reviewed a sample of 34 of the 314 active individual non-employee accounts and determined that 28 accounts (82 percent) were no longer needed but were not disabled until after our audit inquiry. These included badges assigned to former employees, consultants and police officers, as well as three individuals that District officials did not recognize at all.

The 17 shared badges included 10 badges for substitute staff (six for substitute custodians and four for substitute teachers), and seven badges for police and first responders. The head custodians at three buildings were responsible for six shared badges, including three at the middle school, two at the elementary school and one at the high school. The head custodians provided these badges to the substitute custodians at the start of the workday, and the substitute was expected to return it at the end of the workday.

We visited the elementary school custodian office to observe two shared badges assigned to that school. One of the two badges was not found, and the head custodian did not remember what happened to this badge. District officials disabled this badge on May 26, 2026. Subsequently we attempted to locate and observe the custodial shared badges for the middle school and high school; one badge assigned to the middle school was not located and District officials disabled it on May 26, 2026.

District officials did not periodically confirm whether the seven badges were still in the possession of the first responders and needed. Three of these badges were never used, three were last used in 2022, and one was last used in 2020. District officials were not sure whether these badges were still needed and disabled them in May 2026 after confirming first responders had alternative means of access and did not need District-provided badges.

These issues occurred because the District did not have written procedures for staff to follow when requesting a new replacement badge or for tracking and monitoring shared badges. While the badge application form was part of the process, it was not used effectively. In addition, because there was no periodic reconciliation of the badges, District officials were not aware that active badges were missing and therefore did not disable them in a timely manner, increasing the risk of unauthorized and undetected building access.

Account Management and Monitoring Procedures – Although the District had a Board-approved written policy outlining guidelines for issuing employee badges, including temporary badge management (e.g., badges for substitute teachers, volunteers, etc.), returning badges of separated employees, and reporting damaged or lost badges, the policy was adopted in 2013 and was outdated. Furthermore, the policy was not reflective of the process in place during our audit. In addition, the Facilities Department Senior Typist (Typist), who at the time of our audit was responsible for badge management and monitoring was not aware that the policy existed.

The District also did not have any written procedures outlining who is responsible for managing and monitoring accounts. Specifically, District officials did not define who was authorized to create accounts, who was responsible for monitoring active accounts, and the process to revoke access (i.e., deactivating unneeded accounts and collecting badges). The process for adding individual accounts was handled by the Typist who:

- Added accounts for new employees to the system including any access restrictions (e.g., time or a specific entry point) based on the employee's role and required access.
- Added accounts for non-employees including volunteers or contractors.
- Printed and issued prenumbered badges to employees and non-employees.

The Typist used the badge application form, typically completed by the individual needing a badge with an authorization from a department head or District administrator requesting the badge or modifying access. We reviewed the 36 badge application forms for all employee and non-employee badges we sampled previously and observed the back of the form which indicated specific points of entry and a field for an authorizing signature to approve issuing a badge was not completed and was left blank.

During this review, we determined that a badge in the name of a substitute nurse, who left employment on June 30, 2025, was used in August 2025. We determined that the former substitute nurse was providing services as a non-employee contractor to a student attending summer school. Although this individual needed a badge for summer school in 2025, the badge was never returned or disabled. The badge and associated account were not disabled until May 27, 2026 when we brought this to the District officials' attention. Initially, District officials could not easily identify who was using this badge to enter the building because instead of using the badge application form to request the new badge, the Assistant Principal requested the badge verbally in July 2025. Had officials followed policy requirements and used the badge application form there would have been no confusion as to how a former employee was using a badge to gain access to a District building. The badge application form is a key part of the process that supports access management.

The Typist told us she monitored active accounts and was responsible for lost badge deactivation, as well as collecting, deactivating and destroying badges that were no longer needed. She also reissued badges if necessary (e.g., lost or damaged badges). The Typist said there is no formal process for returning a badge or account deactivation. Instead, she relied on the Board meeting minutes, her memory of staffing changes or information provided by Personnel Department staff. However, there are no written procedures or processes for the Personnel Department staff to share staffing changes with the Typist.

Importantly, although the Facilities Department Director had the same administrative rights to the system, the Typist was the only individual adding new accounts and making modifications including activating, deactivating or modifying building access, and no one was providing any oversight or periodically reviewing the Typist's work or the active accounts to determine whether all active accounts were needed. Additionally, the Typist did not use any system reports because she did not receive any training on how to use the system and its functionalities. Due to lack of clear procedures and communication regarding access updates or changes, updates to accounts were not always made in a timely manner and there was a potential for unauthorized access to District buildings.

Recommendations

District officials should:

1. Ensure individuals do not have duplicate accounts and badges.

2. Deactivate accounts and collect the associated badges as soon as they are no longer needed.

3. Develop written procedures that define who is responsible for managing and monitoring accounts including shared badges and periodically evaluate and adjust these procedures to ensure all processes are working as intended.

4. Ensure the badge application form used to request and approve badge issuance is complete and includes proper approval.

5. Develop a reconciliation process utilizing system reports, and review active accounts for necessity and appropriateness of access.

The Board should:

6. Periodically review and update existing policies and ensure they are implemented and complied with.

Appendix A: Profile, Criteria and Resources

Profile

The District's boundaries include the Towns of Milan, Red Hook and Rhinebeck in Dutchess County, and the Towns of Clermont and Livingston in Columbia County. The District's buildings are located on campuses in the Town of Red Hook (elementary and District office, middle school, high school and transportation facility).

The District is governed by the elected seven-member Board. The Board is responsible for managing and controlling the District's financial and educational affairs. The Superintendent is responsible, along with other administrative staff, for managing the District's day-to-day operations under the Board's direction.

The Typist is responsible for managing and monitoring accounts utilizing the system and printing, issuing, and distributing badges. The Facilities Director also has administrative rights to activate, modify and deactivate accounts in the system and performs these functions if the Typist is unavailable.

Criteria

NYSED's Safe Schools by Design Act guidance[2] provides that, as the second line of defense when protecting a building and its occupants, building entry should maintain a welcoming exterior while ensuring safety and security, such as using credentialed electronic access systems. The Cybersecurity and Infrastructure Security Agency's (CISA) K-12 School Security Guide[3] recommends schools should have in place a layered, system-based approach to physical security in which physical security equipment and technology, site and building features, personnel and staff, policies and procedures, and training programs work together to ensure school facilities are secure.

<u>Policies and Procedures</u> – Schools should develop and implement physical security and access control policies and procedures with roles and responsibilities defined and assigned across its organizational entities (e.g., IT, Human Resources (HR), administration, facilities etc.). Policies and procedures should be established to manage, monitor and revoke building access devices and other access credentials as necessary. The policies and procedures should be periodically reviewed and updated to reflect the current and approved access controls implemented within the system and organization.

<u>Building Access/Entry</u> – Schools should control who can enter school buildings, where they can go, and when access is permitted. Building access systems serve as an internal control to help ensure safety and security including controlled entry points, visitor management and monitoring building access. Internal controls over building access/entry should be designed in a way that primary entrances are controlled through device readers, security desks or locked-door systems.

<u>Building Access Account Management</u> – Only designated system users/administrators should be able to create, enable, modify, revoke and remove accounts in accordance with documented policies and procedures. System administrators for access management should be limited and have clearly defined roles and responsibilities. Account management processes should align with individual status changes, such as extended leave, termination or other circumstances when access is not required.

<u>Device Issuance and Authorization</u> – Devices should only be issued with documented approval based on job role and building assignment, each device should be unique and individually assigned. Each individual should only have one device. Shared devices should be avoided so that all activity can be logged to a specific individual. When shared devices must be used a process should be established to track these devices. No

2 https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf
3 https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf

individual should be issued a device until a background check is completed, if required. Visitors and contractors should sign in at a single point of entry and receive a visible identification or badge. Contractors' access should be limited to approved locations and timeframes.

Device Management – Devices should be immediately deactivated when no longer necessary. Any necessary updates to building access should happen promptly. Lost or stolen devices should immediately be reported to staff responsible for deactivating devices and replacement devices should be reissued only with documentation approving the reissuance. Device inventory should be tracked, and periodically reconciled and unused or returned devices should be secured or destroyed.

Building Access Event Monitoring – Device events should be logged by user, door, and timestamp (i.e., device used at door). These logs should be reviewed periodically and/or upon an unauthorized incident. The building access system should generate alerts for after-hours or unauthorized access attempts, if possible. Logs should be retained according to the district policies. Periodically reviewing physical access logs can help identify unexpected activity.

Additional Resources

We also used the following publications to inform our criteria. These publications provide school officials with actionable, practical and cost-effective resources, solutions and tools that enhance school building safety and security:

- **NYSED Safe Schools by Design Act: A Guide by NYSED (April 2025)**
  https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf

- **Partner Alliance for Safer Schools (PASS) Safety and Security Guidelines for K-12 Schools (7th Edition, 2025)**
  https://passk12.org/wp-content/uploads/2025/08/PASS_7thEdition-web.pdf

- **K-12 School Security Guide (3rd Edition, 2022)**
  https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf

- **National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations (Revision 5)**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

In addition, local officials can use our website to search for audits, resources, publications and training for officials at: https://www.osc.ny.gov/local-government

Appendix B: Response From District Officials

The content below is a reproduced copy of the original response letter issued by District officials, is reformatted to meet the Americans with Disabilities Act *Web Content Accessibility Guidelines (WCAG)*,[4] and may have included changes to spelling and grammar. The substance of the content was not changed.

RED HOOK CENTRAL SCHOOL DISTRICT
9 Mill Road, Red Hook, NY 12571
Phone: 845-758-2241
Fax: 845-758-3366

June 20, 2026

Nicole A. Tomsen, Chief of Municipal Audits
Division of Local Government and School Accountability Office of the New York State Comptroller
295 Main Street, Suite 1032
Buffalo, NY 14203-2510
Re: Building Access Audit Report S9-26-7

Dear Ms. Tomsen:

On behalf of the Red Hook Central School District, we acknowledge receipt of the draft audit report regarding Building Access (Report S9-26-7) and appreciate the time and effort invested by the Office of the State Comptroller in conducting this review. We value the recommendations provided and recognize the importance of maintaining effective controls over building access to ensure the safety and security of our students, staff, and visitors.

Since receiving the report and during the audit process, the District has already begun taking steps to strengthen its building access management practices. Initial actions include:

- Reviewing active badge assignments to identify and eliminate duplicate badges where appropriate.
- Conducting a review of non-employee badge holders to verify continued access needs and remove access that is no longer required.
- Reinforcing expectations that badge requests and modifications be documented using existing authorization forms.
- Beginning work on establishing a regular review process for active building access accounts and badge inventories.
- Reviewing current policies and administrative practices to identify areas requiring updates and better alignment with present-day operations.

These efforts represent preliminary measures intended to address immediate concerns and improve oversight of building access accounts and badges. The District is committed to working collaboratively across departments to strengthen internal controls and enhance accountability in this area.

In addition to these actions already underway, the District will develop a comprehensive Corrective Action Plan that addresses each finding and recommendation contained in the audit report. The plan will outline specific corrective measures, responsible parties, and implementation timelines designed to ensure sustained compliance and improved operational effectiveness.

---

4 https://www.ada.gov/resources/2024-03-08-web-rule/#highlights-of-the-requirements-in-the-rule

We appreciate the professional manner in which the audit was conducted and the constructive feedback provided. The District remains committed to continuous improvement and to maintaining a safe and secure environment for our school community.

Warm regards,

Dr. Erin Hayes
Assistant Superintendent for Personnel and Operations

Appendix C: Audit Methodology and Standards

OSC auditors obtained an understanding of internal controls that were deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of the work on internal controls, as well as the work performed in the audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed District officials and reviewed Board policies to gain an understanding of the District's policies, procedures and practices related to managing and monitoring accounts and badges, including roles and responsibilities of the individuals involved in the process.

- We compared the District's 827 active building access accounts list to the employee master file list of 542 employees to determine whether accounts existed that were not associated with current District employees. We interviewed District officials and reviewed relevant documentation to determine whether the accounts and badges assigned to non-employee individuals were necessary. For any unnecessary accounts, we inquired why they were not deactivated.

- We selected all 17 shared accounts and inquired with the District officials responsible for these accounts to observe associated badges to determine whether they were in their possession. If the badges were not in their possession, we inquired as to the reasons why and attempted to locate the badges.

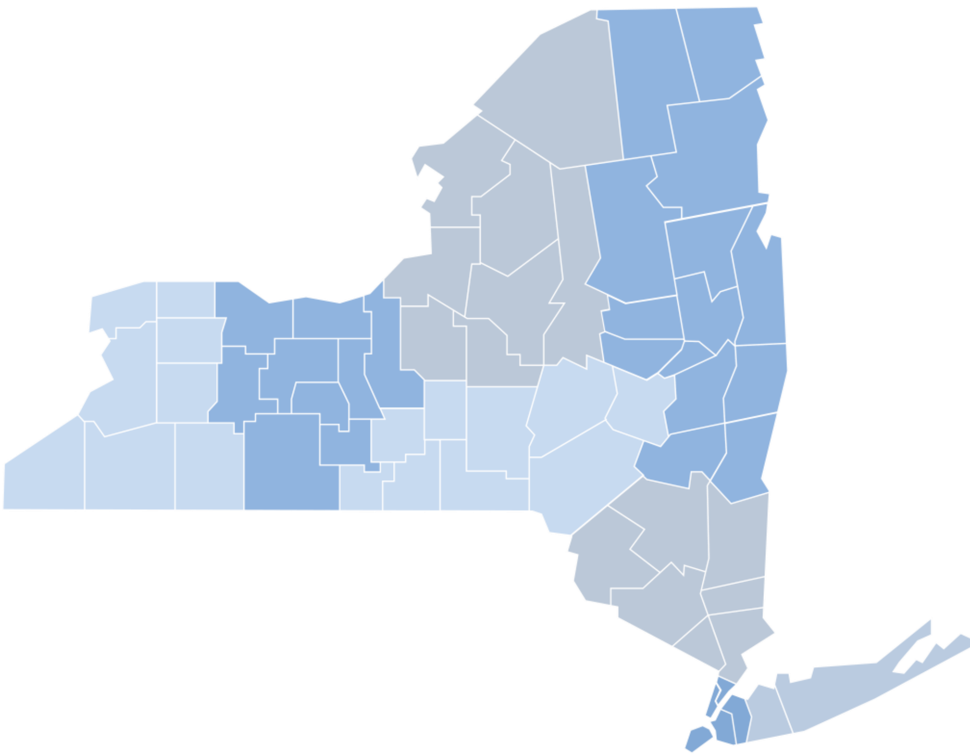
- We reviewed the active building access accounts list to determine whether any individual had more than one account and badge and interviewed District officials to determine why users were assigned more than one badge. We identified 56 individuals (19 non-employees and 37 employees) with a total of 57 duplicate badges. We used our professional judgment to select four employees and four non-employees with two or more active badges totaling 17 badges. We reviewed documentation, including badge application forms, for each individual and interviewed the Typist to determine why they had multiple badges.

OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. Auditors believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected for examination.

Questions?

STATEWIDE AUDITS
Nicole A. Tomsen, Chief of Municipal Audits
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • Fax (716) 847-3643
Email: Muni-Statewide@osc.ny.gov



Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

www.osc.ny.gov

Prepared by the Division of Local Government and School Accountability

FOLLOW US: osc.ny.gov/subscribe